

Experimental implementation of optimal linear-optical controlled-unitary gates

Karel Lemr,^{1,*} Karol Bartkiewicz,^{2,1,†} Antonín Černoš,^{3,‡} Miloslav Dušek,⁴ and Jan Soubusta³

¹*RCPTM, Joint Laboratory of Optics of Palacký University and
Institute of Physics of Academy of Sciences of the Czech Republic,
17. listopadu 12, 771 46 Olomouc, Czech Republic*

²*Faculty of Physics, Adam Mickiewicz University, PL-61-614 Poznań, Poland*

³*Institute of Physics of Academy of Sciences of the Czech Republic,
Joint Laboratory of Optics of PU and IP AS CR,
17. listopadu 50A, 772 07 Olomouc, Czech Republic*

⁴*Department of Optics, Faculty of Science, Palacký University,
17. listopadu 12, cz-77146 Olomouc, Czech Republic*

(Dated: October 17, 2014)

We show that it is possible to reduce the number of two-qubit gates needed for the construction of an arbitrary controlled-unitary transformation by up to two times using a tunable controlled-phase gate. On the platform of linear optics, where two-qubit gates can only be achieved probabilistically, our method significantly reduces the amount of components and increases success probability of a two-qubit gate. The experimental implementation of our technique presented in this paper for a controlled single-qubit unitary gate demonstrates that only one tunable controlled-phase gate is needed instead of two standard controlled-NOT gates. Thus, not only do we increase success probability by about one order of magnitude (with the same resources), but also avoid the need for conducting quantum non-demolition measurement otherwise required to join two probabilistic gates. Subsequently, we generalize our method to a higher order, showing that n -times controlled gates can be optimized by replacing blocks of controlled-NOT gates with tunable controlled-phase gates.

PACS numbers: 42.50.-p, 42.50.Dv, 42.50.Ex

Quantum computing is a promising direction in information processing [1, 2]. Similarly to classical computing, quantum circuits are composed of various elementary gates. In 1989, Deutsch proved the existence of a universal three-qubit gate [3]. Later, DiVincenzo showed that Deutsch's gate can be implemented by a sequence of two- and single-qubit gates [4]. Meanwhile, Barenco discovered a class of two-qubit gates sufficient for building any quantum circuit [5]. A practical set of universal gates was defined later [6]. This set of gates includes several single-qubit gates and only one two-qubit gate — the controlled-NOT (CNOT) gate.

Although the method presented by Barenco *et al.* [6] shows how to construct any quantum circuit, it does not take into account various optimization procedures [7–16]. Optimization is crucial in linear optics, where the CNOT gate can only be implemented probabilistically [17–20], meaning that every repetition reduces the success probability of the entire scheme.

In 2009, Lanyon *et al.* demonstrated a considerable reduction in the number of CNOT gates necessary for circuit construction by introducing additional ancillary modes [21]. They have constructed a Toffoli gate (controlled-controlled-NOT gate) with only two CNOT gates and have also designed a generalized controlled-phase gate, but not an optimal one. Mičuda *et al.* presented a method further reducing resources needed for the implementation of a Toffoli gate to only one CNOT gate [22]. This reduction is achieved by combining po-

larization and spatial encoding to encode a two-qubit state into one single photon. However, the preparation of a specialized control two-qubit state is problematic. It is possible to use quantum routers (or quantum state fusion) [23–25], but this would mean using additional CNOT gates, which would cancel the achieved reduction.

So far only optimizations involving standard CNOT or controlled-sign (c-sign) gates were considered. In 2010, Kielsing *et al.* proposed an optimal (without auxiliary photons) linear-optical implementation of a tunable c-phase gate that imposes a given tunable phase shift φ [26]

$$|kl\rangle \rightarrow e^{i\varphi\delta_{k1}\delta_{l1}}|kl\rangle, \quad (1)$$

where k and l take values of logical qubit states 0 or 1 and δ is the Kronecker's delta. In 2011, the first optimal tunable c-phase gate was experimentally demonstrated [27]. The experiment also allowed to verify and explain the optimal success probability of the gate as a function of the phase shift φ [26, 28].

In this Letter we show that using a tunable c-phase gate instead of a CNOT gate makes it possible to (i) reduce the complexity of various quantum circuits and (ii) increase the success probability of these circuits in linear optics. The support for our idea comes from an experimental implementation of the proposed scheme.

Arbitrary single-qubit controlled-unitary transformation – It has been shown by Barenco *et al.* [6] that two controlled-sign gates are needed to implement an arbitrary controlled-unitary operation acting on a signal

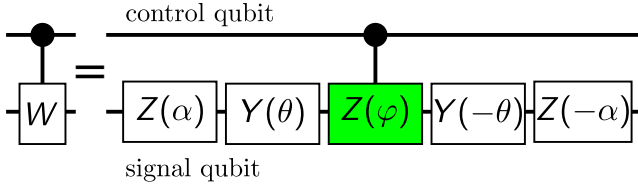


FIG. 1: (color online) Quantum computation circuit implementing an arbitrary single-qubit controlled-unitary operation W [see Eq. (4)] by means of one tunable controlled-phase gate and several unconditional single-qubit operations.

qubit and controlled by a control qubit. In special cases, one controlled-sign gate is sufficient, but at the expense of restricting the class of implemented operations. Considering the probabilistic nature of controlled-sign gates on the platform of linear optics, it is crucial to limit their repetition as much as possible. We show that only one single tunable controlled-phase gate is needed for the construction of a universal single-qubit controlled-unitary operation. Note, that the success probability of two consecutive controlled-sign gates would be $1/81$ (using linear optics only and no photon ancillae), the minimum success probability of a tunable controlled-phase gate is $1/11$ (0.14 on average). Moreover, by reducing the number of gates from two to one, we also avoid the need for intermediary non-demolition presence detection otherwise required to join two probabilistic gates [29, 30].

Let us consider the scheme depicted in Fig. 1. While the upper (control) qubit undergoes only the controlled-phase operation, the lower (signal) qubit is subjected to a set of unconditional single-qubit gates before and after it enters the controlled-phase gate. These unconditional single-qubit gates can be implemented deterministically on the platform of linear optics.

The initial set of single-qubit operations consists of one rotation in z direction

$$Z(\alpha) = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} \quad (2)$$

followed by another rotation in y direction

$$Y(\theta) = \begin{pmatrix} \cos \frac{\theta}{2} & \sin \frac{\theta}{2} \\ -\sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}. \quad (3)$$

Similarly, the single-qubit rotations inserted behind the controlled-phase gate are $Y(-\theta)$ and $Z(-\alpha)$. When the control qubit is $|0\rangle$, the controlled-phase gate does not impose any phase shifts and all unconditional single-qubit rotations cancel each other

$$Z(-\alpha)Y(-\theta)Y(\theta)Z(\alpha) = \mathbb{1}.$$

On the other hand, if the control qubit is $|1\rangle$, the controlled-phase gate introduces an additional rotation in z direction $Z(\varphi)$ [see Eq. (2)]. The overall operation imposed on the signal qubit now reads

$$W = Z(-\alpha)Y(-\theta)Z(\varphi)Y(\theta)Z(\alpha). \quad (4)$$

To demonstrate the universality of the above mentioned gate, let us consider the following: Any single-qubit unitary transformation can be described as a rotation along some axis on the Bloch sphere which corresponds to an operator

$$R_\psi(\varphi) = e^{i\varphi/2}|\psi\rangle\langle\psi| + e^{-i\varphi/2}|\psi^\perp\rangle\langle\psi^\perp|, \quad (5)$$

where φ denotes the rotation angle and $|\psi\rangle$ is the state that geometrically corresponds to the rotation axis on the Bloch sphere ($|\psi^\perp\rangle$ is orthogonal to $|\psi\rangle$). For rotation along the z direction we have $|\psi\rangle = |0\rangle$ which inserted to (4) yields

$$W = Z(-\alpha)Y(-\theta) \left(e^{i\varphi/2}|0\rangle\langle 0| + e^{-i\varphi/2}|1\rangle\langle 1| \right) Y(\theta)Z(\alpha). \quad (6)$$

Using prescriptions (2) and (3) we can easily verify that

$$|\psi\rangle = Z(-\alpha)Y(-\theta)|0\rangle = e^{i\frac{\alpha}{2}} \cos \frac{\theta}{2} |0\rangle + e^{-i\frac{\alpha}{2}} \sin \frac{\theta}{2} |1\rangle, \quad (7)$$

and thus show that any arbitrary pure qubit state is accessible if suitable values of α and θ are set. Unitary transformations maintain orthogonality so that $|1\rangle \rightarrow Z(-\alpha)Y(-\theta)|1\rangle = |\psi^\perp\rangle$. The two pairs of unconditional single-qubit rotations before and after the c -phase gate permit for any rotation axis. Tuning the phase of the c -phase gate permits for setting any rotation angle φ .

Any single-qubit unitary operation can be decomposed in the form of [6]

$$U = Z(\gamma)Y(\omega)Z(\delta) \quad (8)$$

parametrized by three real numbers. An explicit decomposition of the transformation matrix can be found in the Supplementary material [31]. Note that the matrix W in (4) is also parametrized by three real numbers. Optimality of our method is guaranteed by the fact that we only use one probabilistic gate which is optimal for any given phase shift required by the transformation.

Experimental implementation – We have constructed an experimental setup as depicted in Fig. 2. It consists of a tunable c -phase gate placed between single-qubit gates in the signal mode that implement the required unconditional rotations Z and Y . In our experiment we encode qubits into polarization states of individual photons ($|0\rangle$ corresponds to horizontal polarization $|H\rangle$, $|1\rangle$ to vertical polarization $|V\rangle$). Unconditional single-qubit rotations Z and Y are implemented by sets of one half- and one quarter-wave plates. The control state preparation is achieved by one half-wave plate in control mode since only logical states $|0\rangle$ and $|1\rangle$ are required. Photons were generated using Type I spontaneous parametric down-conversion in a LiIO_3 crystal pumped by 200 mW cw Kr^+ laser beam. By following the procedure described in Ref. [27], we have adjusted the tunable c -phase gate to a given phase shift φ .

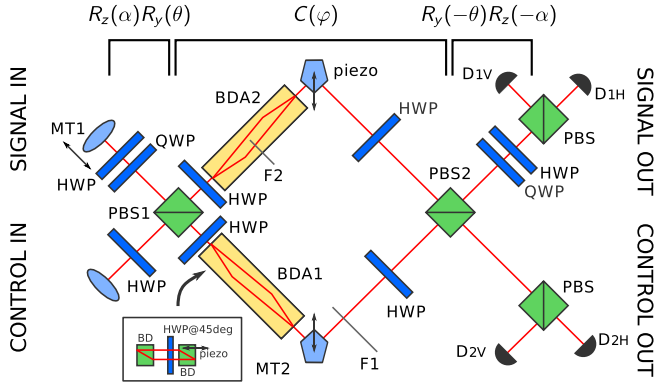


FIG. 2: (color online) Schematic drawing of the experimental setup. The components are labeled as follows: MT – motorized translation, HWP – half-wave plate, QWP – quarter-wave plate, PBS – polarizing beam splitter, BDA – beam divider assembly, BD – beam divider, D – detector.

We have tested our device on six combinations of tunable c-phase gate phase shifts φ and single qubit rotations $Z(\alpha)$ and $Y(\theta)$ (see Tab. I). In all these six cases, we have performed complete process tomography of the signal mode for the control qubit set to state $|0\rangle$ and then also to $|1\rangle$ [32–35]. The estimated Choi matrices were compared to theoretical predictions permitting to calculate their fidelities \mathcal{F} and purities \mathcal{P} . We adopt the following labeling: \mathcal{F}_{off} and \mathcal{P}_{off} stand for fidelity and purity observed with control qubit set to $|0\rangle$, while \mathcal{F}_{on} and \mathcal{P}_{on} denote the same parameters for control qubits in the state $|1\rangle$. We have also determined the resulting success probabilities by comparing the coincidence rate observed after adjusting the gates with the coincidence rate behind the same setup, but with all filters removed and polarizations set so that no single or two-photon interference takes place. Thus, we obtain the experimental success probability p_{succ} corrected for “technological losses” (e.g. components back-reflections or coupling losses). The results of our experiment are summarized in Tab. I and one selected case is also depicted in Fig. 3. Estimated fidelities and purities are typically about 90% which indicates good agreement with theoretical predictions.

n-times controlled single qubit unitary transformations

– As in case of a CNOT gate, a Toffoli gate (CCNOT) can be used to implement a controlled unitary gate, but with two control qubits. The CCNOT operation can be implemented using only CNOT gates. We can also build a 2-times controlled gate by replacing the CNOT gates acting on the target qubit with c-phase gates and single-qubit rotations. This approach ensures efficiency higher than in case of a circuit using only CNOTs, where CNOT gates modifying the target qubit are each replaced with a single-qubit rotation sandwiched between two CNOT gates. This means the latter approach is equivalent to adding 3 two-qubit gates to the circuit proposed in Lemma 6.1 in Ref. [6].

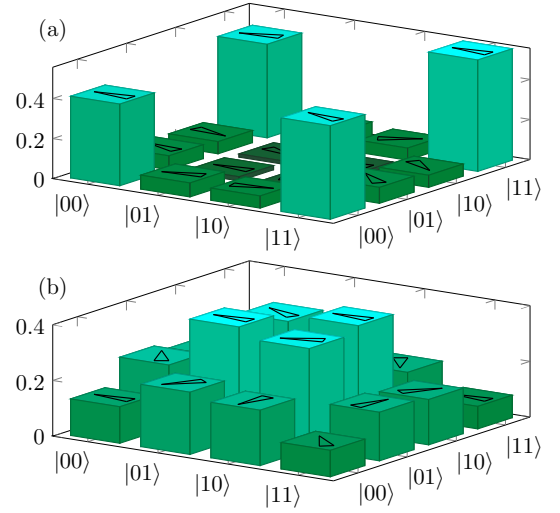


FIG. 3: (color online) Estimated process matrices for $\varphi = \frac{3\pi}{4}$, $\theta = \frac{\pi}{2}$ and $\alpha = 0$ (a) with control qubit $|0\rangle$ and (b) with control qubit $|1\rangle$. Moduli of matrix elements are visualized by bar heights and their phase by arrow directions.

The situation is analogous for any n -times controlled unitary gate. Designing an arbitrary n -times controlled gate is usually considered in the context of Toffoli gates. However, constructing such circuits directly with Toffoli gates has been proven inefficient as it needs an order of n^2 two-qubit gates [1]. It has been demonstrated that, by extending the Hilbert space of the target information carrier (see Ref. [21]), one can implement an arbitrary n -times controlled gate by using $2n - 1$ standard two-qubit gates performing controlled-Pauli operations ($R_n(\pi)$ for $n = x, y, z$). This is considered to be the most effective currently known solution.

In linear optics we can increase the efficiency of an n -times controlled unitary gate proposed by Lanyon *et al.* [21] by replacing two standard controlled-Pauli gates with a controlled-unitary operation performed with higher probability of success. In the original scheme, the authors of Ref. [21] show that any n -qubit controlled gate can be implemented using only $2n$ CNOT gates and single-qubit operations. Similarly, we show in Fig. 4 any n -times controlled- U gate can be reduced to $2(n - 1)$ CNOT gates and one single-qubit controlled-phase gate. This is possible by using $(n + 1)$ -level system as the bottom-most circuit line. This reduces the number of the required two-qubit gates by one, and has the additional merit in having the single qubit controlled- U gate work with a higher average success probability than a CNOT gate.

This optimization can be applied in a linear-optical implementation of the 2-times controlled unitary gate from Ref. [21]. The improvement is apparent if we consider replacing the product of CNOT, CZ and R gates by a product of two controlled-unitary gates and single-qubit

TABLE I: Experimental results for various settings of the c-phase gate parameter φ together with single qubit rotations α and θ . The corresponding values of standard decomposition parameters ω , γ and δ are also calculated. \mathcal{F}_{off} and \mathcal{P}_{off} denote estimated process fidelity and purity of the transformation with the control qubit set to $|0\rangle$, while \mathcal{F}_{on} and \mathcal{P}_{on} denote the same characteristics with the control qubit set to $|1\rangle$. p_{succ} and p_{succTH} stand for experimental and theoretical success probability.

φ	θ	α	ω	γ	δ	\mathcal{F}_{off}	\mathcal{P}_{off}	\mathcal{F}_{on}	\mathcal{P}_{on}	p_{succ}	p_{succTH}
0	0	0	0	0	0	0.964 ± 0.001	0.940 ± 0.001	0.971 ± 0.001	0.957 ± 0.001	0.822 ± 0.059	1.000
$\pi/8$	$\pi/2$	0	$\pi/8$	$\pi/2$	$-\pi/2$	0.973 ± 0.001	0.981 ± 0.003	0.918 ± 0.002	0.912 ± 0.005	0.180 ± 0.008	0.210
$\pi/4$	0	$\pi/2$	0	$\pi/8$	$\pi/8$	0.928 ± 0.003	0.921 ± 0.005	0.878 ± 0.004	0.863 ± 0.006	0.105 ± 0.017	0.133
$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$	0	0	0.900 ± 0.004	0.909 ± 0.006	0.909 ± 0.004	0.913 ± 0.007	0.086 ± 0.005	0.090
$3\pi/4$	$\pi/2$	0	$3\pi/4$	$\pi/2$	$-\pi/2$	0.937 ± 0.003	0.950 ± 0.006	0.889 ± 0.004	0.909 ± 0.007	0.079 ± 0.006	0.088
π	0	$\pi/2$	0	$\pi/2$	$\pi/2$	0.934 ± 0.004	0.936 ± 0.006	0.771 ± 0.005	0.833 ± 0.007	0.108 ± 0.016	0.111

operations. The product of two controlled-unitary gates works on average with a higher success rate than a product of CZ and CNOT gates. Hence, by using an optimal implementation of a c-phase gate, we can increase the success rate of the circuit by approximately one order of magnitude.

The currently known most efficient implementation of the Toffoli gate in terms of the number of two-qubit gates was presented by Mićuda *et al.* in Ref. [22]. This approach requires only one CZ gate. However, it is possible to obtain an even more efficient circuit for the controlled- U if we replace the CZ with a c-phase gate instead of the product of two CNOTs and single-qubit rotations.

Any n -times controlled operation can be constructed from Toffoli gates and a single-qubit controlled unitary gate regardless of the auxiliary resources. Therefore, we infer that our reasoning and the resulting improvement is valid for all implementations of the CCNOT.

Conclusions — We have presented a method for the optimization of quantum circuits based on a tunable c-phase gate. This method decreases the number of controlled operations needed in circuit design and significantly increases the success probability on physical platforms where controlled gates can only be implemented probabilistically (e.g. linear optics). Moreover, the reduction in number of gates makes circuits less complex and thus more experimentally accessible. We have demonstrated the experimental feasibility of our approach on the basis of one experimental case, namely the single-qubit controlled-unitary operation.

Acknowledgements — The authors thank Jára Cimrman for his helpful suggestions. K. L. acknowledges support by Czech Science Foundation (Grant No. 13-31000P). A. Č. acknowledges support by Czech Science Foundation (Grant No. P205/12/0382). K. B. acknowledges support by the Foundation for Polish Science and the Polish National Science Centre under grant No. DEC-2013/11/D/ST2/02638, the Operational Program Research and Development for Innovations European Regional Development Fund (Project No. CZ.1.05/2.1.00/03.0058) and Operational Program Education for Competitiveness European Social Fund (Project No. CZ.1.07/2.3.00/20.0017) of the Ministry

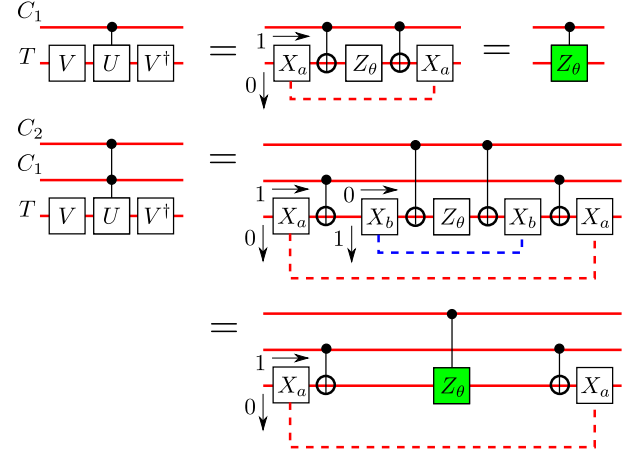


FIG. 4: (color online) 2-times and 3-times c-phase $[Z(\theta)]$ gates decomposed with a method of Lanyon *et al.* [21] based on extending the Hilbert space of the target qubit. The control lines are denoted as C_n for $n = 1, 2, 3$ and T denotes the target qubit line. For the 2(3)-times controlled gate the dimension of the target qubit is extended by 1(2). The additional dimensions are visualized as additional dashed channels. For technical details on operation of X_a and X_b gates see Ref. [21]. By iterating the depicted procedure for an n -times controlled gate we conclude that $2(n-1)$ CNOTs and a single c-phase are needed for its implementation. An arbitrary controlled- U gate, where $U = V^\dagger Z_\theta V$ can be easily implemented using the same circuits by applying V and V^\dagger single-qubit operations.

of Education, Youth and Sports of the Czech Republic. M. D. acknowledges support from the Palacký University (IGA-PrF-2014008).

Supplementary material

Decomposition of single-qubit controlled-unitary operation

We have demonstrated in the text, that the set of gates depicted in Fig. 1 (in the main text) allows to implement any controlled-unitary transformation in the signal qubit mode. The overall operation of the gates on the signal

qubit can be described by the matrix

$$W = Z(-\alpha)Y(-\theta)Z(\varphi)Y(\theta)Z(\alpha). \quad (9)$$

It is however customary to decompose the desired unitary transformations in the form of

$$U = Z(\gamma)Y(\omega)Z(\delta). \quad (10)$$

In this section, we find analytical formulas allowing to map the set of parameters $\{\alpha, \theta, \varphi\}$, used in the matrix W describing our scheme, to the set of decomposition parameters $\{\gamma, \omega, \delta\}$. Let us now express both the transformations U and W in matrix forms using definitions introduced in the main text.

Firstly, we write the form of matrix W in a compact form as follows

$$W = \begin{pmatrix} \chi & \xi \\ -\xi^* & \chi^* \end{pmatrix}, \quad (11)$$

where we introduced two auxiliary parameters

$$\chi(\theta, \varphi) = e^{-i\varphi/2} \cos^2 \frac{\theta}{2} + e^{i\varphi/2} \sin^2 \frac{\theta}{2} \quad (12)$$

and

$$\xi(\alpha, \theta, \varphi) = e^{i(\alpha - \frac{\pi}{2})} \sin \theta \sin \frac{\varphi}{2}. \quad (13)$$

Secondly, we derive the matrix form of the decomposed unitary transformation

$$U = \begin{pmatrix} e^{-i\frac{\gamma+\delta}{2}} \cos \frac{\omega}{2} & e^{i\frac{-\gamma+\delta}{2}} \sin \frac{\omega}{2} \\ -e^{i\frac{\gamma-\delta}{2}} \sin \frac{\omega}{2} & e^{i\frac{\gamma+\delta}{2}} \cos \frac{\omega}{2} \end{pmatrix}. \quad (14)$$

Our goal is now to find a unique relation between both sets of three parameters, that guarantee equivalence $U(\gamma, \omega, \delta) = W(\alpha, \theta, \varphi)$.

We start by comparing the amplitudes of the individual terms of the matrices. One can straightforwardly identify

$$\cos \frac{\omega}{2} = |\chi| \quad (15)$$

and simultaneously

$$\sin \frac{\omega}{2} = |\xi|. \quad (16)$$

Since the relation $|\chi|^2 + |\xi|^2 = 1$ holds disregarding the values of φ and θ , one can always fulfil both conditions (15) and (16) simultaneously. These equations allow to calculate parameter ω

Analysing the phases of the diagonal and offdiagonal terms directly reveals that

$$\delta + \gamma = -2\angle(\chi), \quad (17)$$

respectively

$$\delta - \gamma = 2\alpha - \pi. \quad (18)$$

This set of two equations can be easily solved obtaining both γ and δ as functions of α and $\angle(\chi)$, that is the polar angle of the complex number χ .

It is fair to derive also inverse relations between both sets of parameters. By directly comparing the real part of χ with the real part of the corresponding term in U , we obtain

$$\cos \frac{\varphi}{2} = \cos \frac{\gamma + \delta}{2} \cos \frac{\omega}{2}. \quad (19)$$

Comparing the imaginary part of χ with the imaginary part of corresponding term in U and using (19) one finds the second inverse relation

$$\cos \theta = \frac{\sin \frac{\gamma+\delta}{2} \cos \frac{\omega}{2}}{\sqrt{1 - \cos^2 \frac{\gamma+\delta}{2} \cos^2 \frac{\omega}{2}}}. \quad (20)$$

Finally, from (18) it is trivial to derive the last inverse relation

$$\alpha = \frac{\delta - \gamma + \pi}{2}. \quad (21)$$

Experimental implementation and results

In our experiment we encode qubits into polarization state where $|0\rangle$ corresponds to horizontally polarized $|H\rangle$ and similarly $|1\rangle$ corresponds to vertical polarization $|V\rangle$. We have constructed the experimental setup as shown in Fig. 2 in the main text. This setup consists of a tunable c-phase gate enveloped in the signal mode by single qubit transformations used to set required unconditional rotations $Z(\pm\alpha)$ and $Y(\pm\theta)$. These rotations are implemented by sets of one half-wave plate and one quarter-wave plate inserted in front and behind the c-phase gate. The control state preparation is achieved by individual half-wave plate in the control mode since only logical states $|1\rangle$ and $|0\rangle$ are required to switch the unitary operation on the signal qubit on and off.

In order to simplify the experimental scheme and to limit the number of required wave plates, we used only one set of half and quarter-wave plates in front of the c-phase gate to set the rotations $Z(\alpha)$ and $Y(\theta)$ and in the same time to adjust required input state. Similarly, the half and quarter-wave plates behind the c-phase gate are used to implement both the rotations $Z(-\alpha)$ and $Y(-\theta)$ and to accomplish polarization projection required for the complete process tomography of the signal mode.

We tested the operation of our device for six different settings of the parameters $\{\alpha, \theta, \varphi\}$. The results of our experiments were summarized in Tab. 1 in the main text, where we listed estimated fidelities and purities, that are typically about 90%. Due to the limited space of the main text we plot examples of the experimental estimated and theoretical matrices of the controlled-unitary operation in this section in Fig. 5. The plotted diagrams indicate

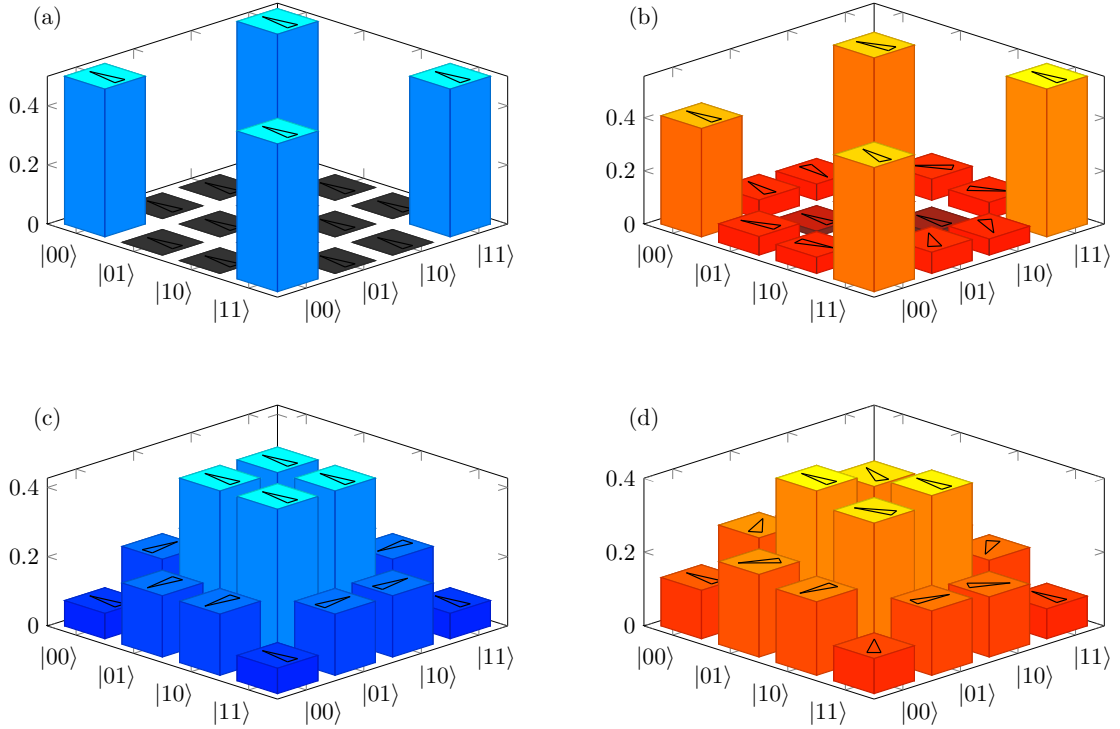


FIG. 5: (color online) Estimated process matrices of controlled-unitary operation with $\varphi = \frac{3\pi}{4}$, $\theta = \frac{\pi}{2}$ and $\alpha = 0$: (a) theoretical prediction with control qubit set to $|0\rangle$, (b) experimental implementation with control qubit set to $|0\rangle$, (c) theoretical prediction with control qubit set to $|1\rangle$, (d) experimental implementation with control qubit set to $|1\rangle$. Bar height represents the modulus of the matrix element and the black arrow on it's top visualize phase shift of that particular matrix element.

very good agreement of our experiment with the theoretical predictions.

* Electronic address: k.lemr@upol.cz

† Electronic address: bartkiewicz@jointlab.upol.cz

‡ Electronic address: acernoch@fzu.cz

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
- [2] D. Bouwmeester, A. Ekert, A. Zeilinger, *The Physics of Quantum Information*, Springer, Heidelberg, 2001.
- [3] D. Deutsch, Proc. Roy. Soc. London A **425**, 73 (1989).
- [4] D. P. DiVincenzo, Phys. Rev. A **51**, 1051 (1995).
- [5] A. Barenco, Proc. Roy. Soc. London A **449**, 679 (1994).
- [6] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457–3467 (1995).
- [7] S. S. Bullock, I. L. Markov, *Proceedings of the 40th conference on design automation (ACM Press)*, 324–329 (2003).
- [8] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. Lett. **91**, 027903 (2003).
- [9] V. V. Shende, I. L. Markov, and S. S. Bullock, Phys. Rev. A **69**, 062321 (2004).

- [10] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. Lett. **92**, 177902 (2004).
- [11] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Phys. Rev. Lett. **93**, 130502 (2004).
- [12] F. Vatan, C. Williams, arXiv:quant-ph/0308006v1
- [13] G. Vidal and C. M. Dawson, Phys. Rev. A **69**, 010301(R) (2004).
- [14] V. Bergholm, J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. A **71**, 052330 (2005).
- [15] V. V. Shende, S. S. Bullock, I. L. Markov, IEEE Trans. on Computer-Aided Design **25**, 1000–1010 (2006).
- [16] M. Plesch and Č. Brukner, Phys. Rev. A **83**, 032302 (2011).
- [17] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **66**, 024308 (2002).
- [18] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White, Phys. Rev. Lett. **95**, 210504 (2005).
- [19] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, Phys. Rev. Lett. **95**, 210505 (2005).
- [20] M. Bartkowiak and A. Miranowicz, J. Opt. Soc. Am. B **27**, 2369–2377 (2010).
- [21] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, Nat. Physics **5**, 134–140 (2009).
- [22] M. Mičuda, M. Sedlák, I. Straka, M. Miková, M. Dušek, M. Ježek, and J. Fiurášek, Phys. Rev. Lett. **111**, 160407 (2013).

- (2013).
- [23] K. Lemr, A. Černoch, Opt. Comm. **300**, 282–285 (2013).
 - [24] K. Lemr, K. Bartkiewicz, A. Černoch, J. Soubusta, Phys. Rev. A **87**, 062333 (2013).
 - [25] C. Vitelli, N. Spagnolo, L. Aparo, F. Sciarrino, E. Santamato, L. Marrucci, Nat. Photon. **7**, 521 (2013).
 - [26] K. Kieling, J. L. O’Brien, J. Eisert, New J. Phys. **12**, 013003 (2010).
 - [27] K. Lemr, A. Černoch, J. Soubusta, K. Kieling, J. Eisert, and M. Dušek, Phys. Rev. Lett. **106**, 013602 (2011).
 - [28] K. Lemr and A. Černoch, Phys. Rev. A **86**, 034304 (2012).
 - [29] P. Kok, H. Lee, and J. P. Dowling, Phys. Rev. A **66**, 063814 (2002).
 - [30] M. Bula, K. Bartkiewicz, A. Černoch, K. Lemr, Phys. Rev. A **87**, 033826 (2013).
 - [31] See Supplementary material at <http://> for more details.
 - [32] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972)
 - [33] M.-D. Choi, Lin. Alg. Appl. **10**, 285–290 (1975).
 - [34] M. Ježek, J. Fiurášek, and Z. Hradil, Phys. Rev. A **68**, 012305 (2003).
 - [35] M. G. A. Paris and J. Řeháček (Eds.), *Quantum State Estimation*, Lect. Notes Phys. **649**, (Springer, Berlin, Heildeberg, 2004).